FROST & SULLIVAN



National Government Communication Modernization: Solving the Constraint-Management Challenge

FROST & SULLIVAN VBOOK

The contents of these pages are copyright © Frost & Sullivan. All rights reserved.

CONTENTS

3 Government's New Operating Burden

4 Fragmentation Is the Primary Constraint on Coordination

5 Resilience Has Been Redefined by Failure

6 Sovereignty Defines What Can Be Procured

7 Hybrid Architecture Is the Logical Convergence Point

8 The Workforce Model Is Misaligned with the Tools Supporting It

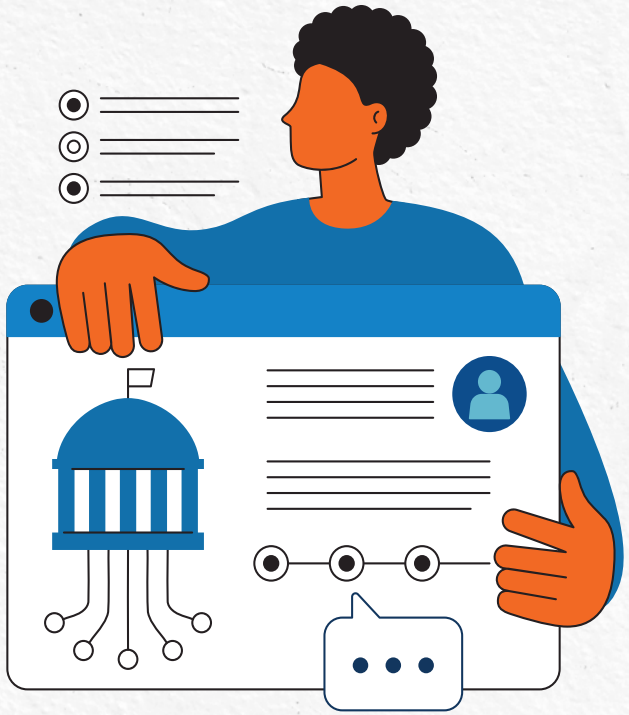
10 AI Needs an Operating Model, Not Just a Use Case

11 Communications Investment Determines Government Operating Capability

13 Complexity Has Become the Next Modernization Constraint

14 Choosing the Right Partner for Scalable, Secure Transformation

15 Mitel in Practice



Government's New Operating Burden

A structural shift is underway in national and federal governments, one that is often acknowledged but not fully internalized. Historically, national and federal institutions were designed to define and administer policy, such as processing taxes, adjudicating claims, and regulating industries. Today, that mandate has expanded. Governments are now expected to operate continuously, coordinating across ministries, managing national-scale services, and responding dynamically to crises that cut across borders, agencies, and domains.

This shift introduces a fundamental mismatch. The communications infrastructure underpinning government operations was not designed for persistent, real-time coordination at such a scale. The result is not simply inefficiency; it is a structural friction between what governments are expected to do and what their infrastructure enables them to do.

While the front-end websites and apps look modern, the back-end infrastructure and collaboration networks are frequently suffocating under legacy technical debt.

- The UN's 2024 E-Government Survey shows 189 of 193 countries now offer online transactional services,[1] as portals evolve into always-on infrastructure.
- However, the US Government Accountability Office (GAO) reports that of the federal government's $100B+ annual IT spend, up to 80% is consumed by Operating & Maintaining (O&M) legacy systems, some of which are 30 to 50 years old.[2]
- The UK Central Digital and Data Office estimates that 28% of systems in central government departments in 2024 were legacy systems, a rise from the 2023 figure of 26%.[3]

As governments are asked to coordinate continuously, respond faster, and deliver national-scale services in real time, outdated communications estates increasingly determine what is possible, what is delayed, and where resilience breaks under pressure.

[1] United Nations E-Government Survey 2024, https://www.un-ilibrary.org/content/books/9789211067286

[2] US Government Accountability Office (GAO): Information Technology: Agencies Need to Fully Implement Key Practices for Legacy System Modernization, July 2025

[3] State of digital government review, Secretary of State for Science, Innovation and Technology by Command of His Majesty, January 2025

Fragmentation Is the Primary Constraint on Coordination

Most central government environments are aggregations, not unified systems. Ministries, agencies, and sub-national entities typically operate distinct communication platforms: legacy telephony in some areas, modern unified communications (UC) in others, and ad-hoc integrations bridging the gaps. Over time, this effectively creates a federated but not interoperable estate.

This fragmentation is not accidental. It is reinforced by procurement structures, funding models, and jurisdictional autonomy. In many countries, a significant proportion of public procurement occurs outside centralized control, limiting standardization and interoperability across organizations.

Without a built-in system for coordination, teams are forced to rely on ad hoc workarounds and manual intervention. While this causes minor friction day-to-day, it becomes a severe liability during a national crisis.

Fragmentation is a coordination risk embedded in the government operating model, not a narrow IT issue.

IT decision-makers from government institutions identified the following top employee communication challenges for their organization:



Resilience Has Been Redefined by Failure

Government expectations of resilience have shifted materially over the past decade as a series of high-profile infrastructure failures and major digital program challenges exposed risks inherent to highly centralized architectures. While centralization can deliver efficiency in cost, management, and standardization, it concentrates operational risk. When critical services depend on a single platform, provider, or communications pathway, a single technical failure can rapidly propagate into a national-scale service disruption. This has prompted governments to reconsider the assumption that cloud-first or otherwise centralized architectures are inherently resilient for sensitive or mission-critical workloads.

The failure of the UK Emergency Call Handling Service in June 2023 illustrates this risk. A technical fault disrupted access to the 999 and 112 emergency numbers across the United Kingdom for approximately 10.5 hours. As 999 and 112 calls route directly to police, fire, and ambulance dispatch, the outage put public safety response at risk alongside the underlying technology failure, underscoring the stakes for mission-critical dispatch and emergency communications capability. Because all emergency calls were routed through a single national platform, the outage exposed how centralized architectures can create a systemic single point of failure, demonstrating that the resilience of essential government services depends not only on the reliability of individual components but also on the architectural diversity and redundancy of the system as a whole.

Resilience is no longer defined by uptime metrics alone. It is defined by the operating layer's capability to remain operationally intact under stress. In response, government IT decision-makers are prioritizing the following investments as "Crucial and Very Important" over the next 2–3 years.



Resilience is tested continuously under real-world conditions, not proven in theory.

Sovereignty Defines What Can Be Procured

Government buyers are increasingly constrained by regulatory and security frameworks that define requirements for data residency, operational control, legal jurisdiction, and governance. Solutions that cannot demonstrate compliance with these mandatory criteria are unlikely to progress through procurement, regardless of their technical capabilities.

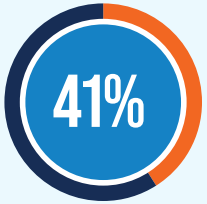
This introduces a second-order challenge. Many modern communication platforms are built on globally distributed cloud architectures. While sovereign cloud offerings may address data residency requirements, they do not necessarily provide equivalent assurance over administrative control, foreign legal exposure, or operational governance. Governments must therefore evaluate sovereignty across multiple dimensions rather than approaching it as a single technical attribute.

Sovereignty has consequently evolved from a policy aspiration into a procurement gate that shapes which solutions can be considered, how they are evaluated, and ultimately which technologies can be deployed.

Data sovereignty is an important factor for a combined 97% of government IT decision-makers when purchasing communications and collaboration software, services, and infrastructure over the next 3 years.



Must have it



Would like to have it



Can live without it

If a solution cannot meet sovereignty requirements, it is not included in the decision set.

Hybrid Architecture Is the Logical Convergence Point

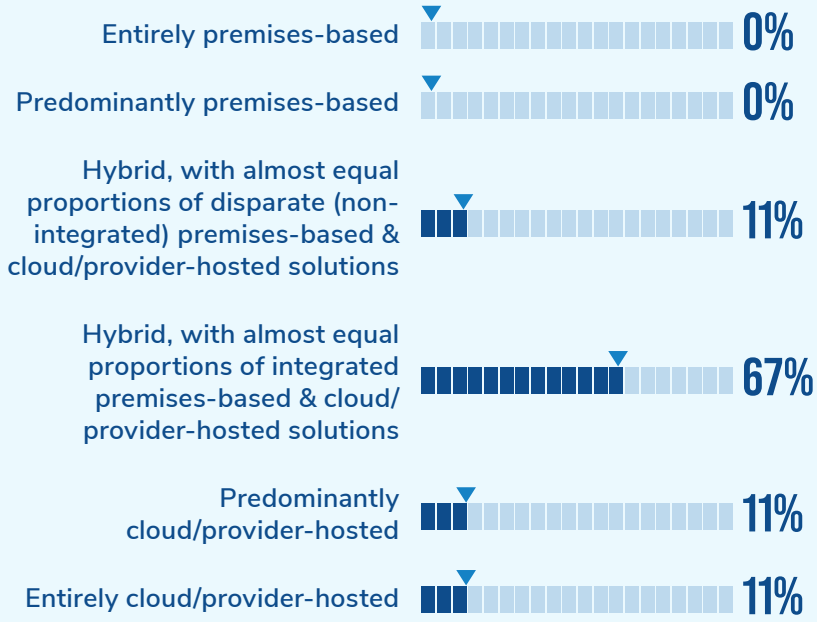
Given the constraints of fragmentation, resilience requirements, and sovereignty, government infrastructure is converging toward hybrid architectures. This operational model represents a permanent steady state, rather than a temporary transition.

Hybrid environments allow governments to retain control over sensitive workloads through on-premises or private infrastructure, while selectively leveraging cloud-based capabilities for scalability and the processing power required for AI and analytics. Critically, hybrid approaches align with how governments procure and modernize incrementally, within defined budget cycles, and without large-scale disruption. The alternative, wholesale replacement, rarely aligns with operational, financial, or political realities.

Hybrid architecture has long-term viability not because government is indecisive, but because it is the only model capable of reconciling operational continuity, sovereignty, resilience, and incremental modernization.

Government IT decision-makers recognize the advantages of a hybrid estate: the incremental modernization capability aligns with procurement cycles, integration with existing infrastructure investments, and controlled adoption of advanced functionalities.

The 2029 Government Call/Telephony Environment Landscape



Moving toward a hybrid estate directly solves the modernization puzzle for government IT decision-makers. Step-by-step upgrades fit neatly into established procurement cycles, existing infrastructure investments stay protected, and advanced functionalities can be rolled out on a controlled, manageable schedule.

The Workforce Model Is Misaligned with the Tools Supporting It

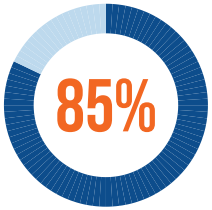
National and federal government communication transformation is often framed as a challenge of platforms, applications, and infrastructure. But government outcomes are delivered by people, often far from desks and under real operational pressure. Border officers processing arrivals, inspectors conducting field assessments, benefits caseworkers supporting citizens, emergency dispatchers coordinating multi-agency response, and first responders making time-critical decisions all depend on communications that work at the point of execution.

However, most communications environments are optimized for desk-based knowledge workers around fixed locations, application-led interactions, and tolerable delays in communication and decision-making. Frontline government works differently. Decisions are made under pressure and with little tolerance for latency. When information fails to reach the right person quickly, the execution gap becomes an operational risk.

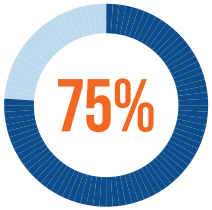
This approach is not aspirational. It is already being implemented in safety-critical environments. For example, a national rail infrastructure organization responsible for public safety across thousands of miles of railway partnered with Mitel to deploy a safety-critical communications solution linking signalers with workers across the network. The platform provides precise caller location information, enabling rapid, informed decisions and immediate action when risks arise. Here, communication is not a support function, but a mission-critical capability that underpins safety, operations, and the protection of lives.



A cascading proportion of government IT decision-makers state CPaaS and API-enabled communication use cases are “Crucial or Very Important” over the next 3 years, including:



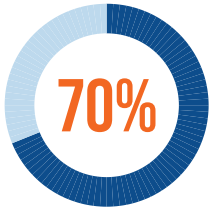
Integrating communications (voice, messaging, video) into business applications



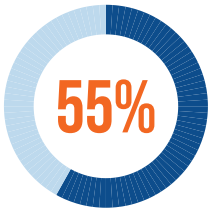
Strengthening security & trust



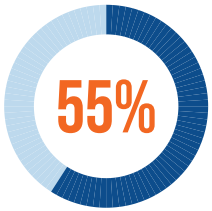
Enabling automation & AI-driven workflows



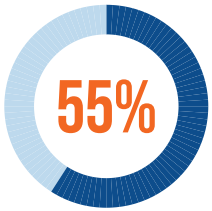
Supporting global communications reach & local regulatory compliance



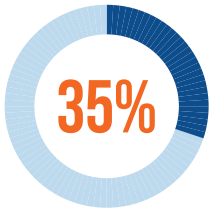
Customizing employee or frontline worker communications & collaboration experiences



Improving customer engagement



Enhancing analytics, monitoring, or performance visibility across communications & networks



Adding digital channels

Government transformation succeeds or fails at the point of execution, where frontline workers must act on information rather than simply access it.

AI Needs an Operating Model, Not Just a Use Case

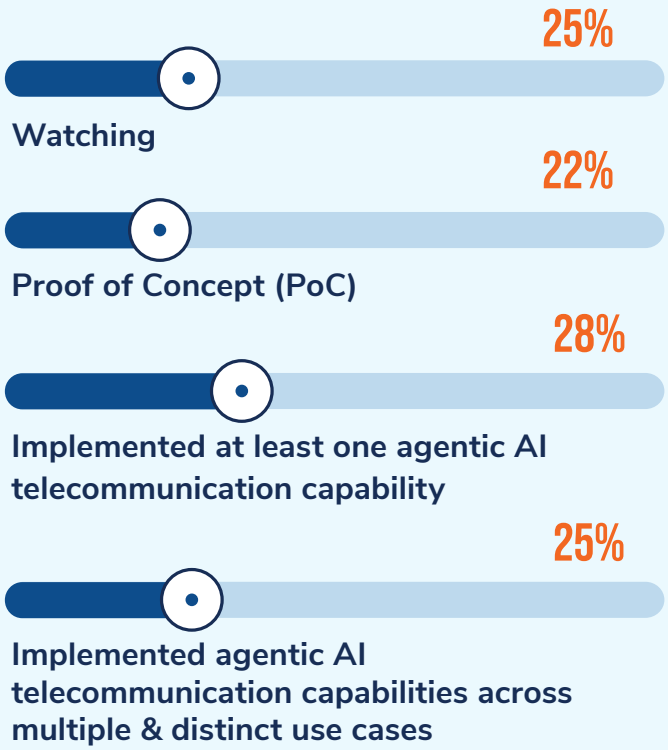
Artificial intelligence has become a strategic priority across government. Yet, while pilot projects and isolated use cases continue to multiply, scaled deployment remains comparatively rare. The challenge is not a lack of interest in AI. It is that AI magnifies the strengths and weaknesses of the environment in which it operates.

AI requires trusted communications channels, stable and resilient infrastructure, interoperable systems, governed data flows, and clearly defined operational processes.

Organizations that approach AI as a standalone technology initiative risk creating a collection of disconnected tools. Organizations that integrate AI as part of a broader operating model can embed intelligence directly into decision-making, workflow automation, citizen engagement, and operational coordination.

AI readiness is fundamentally an operating model challenge, not a technology procurement challenge.

For government organizations, the AI challenge is less about generating interest and more about advancing maturity. While three out of four organizations have reached at least the proof-of-concept stage, only one in four have deployed agentic AI across multiple, distinct use cases. This gap highlights the real challenge of establishing an operating model that enables these deployments to scale safely, consistently, and coherently.



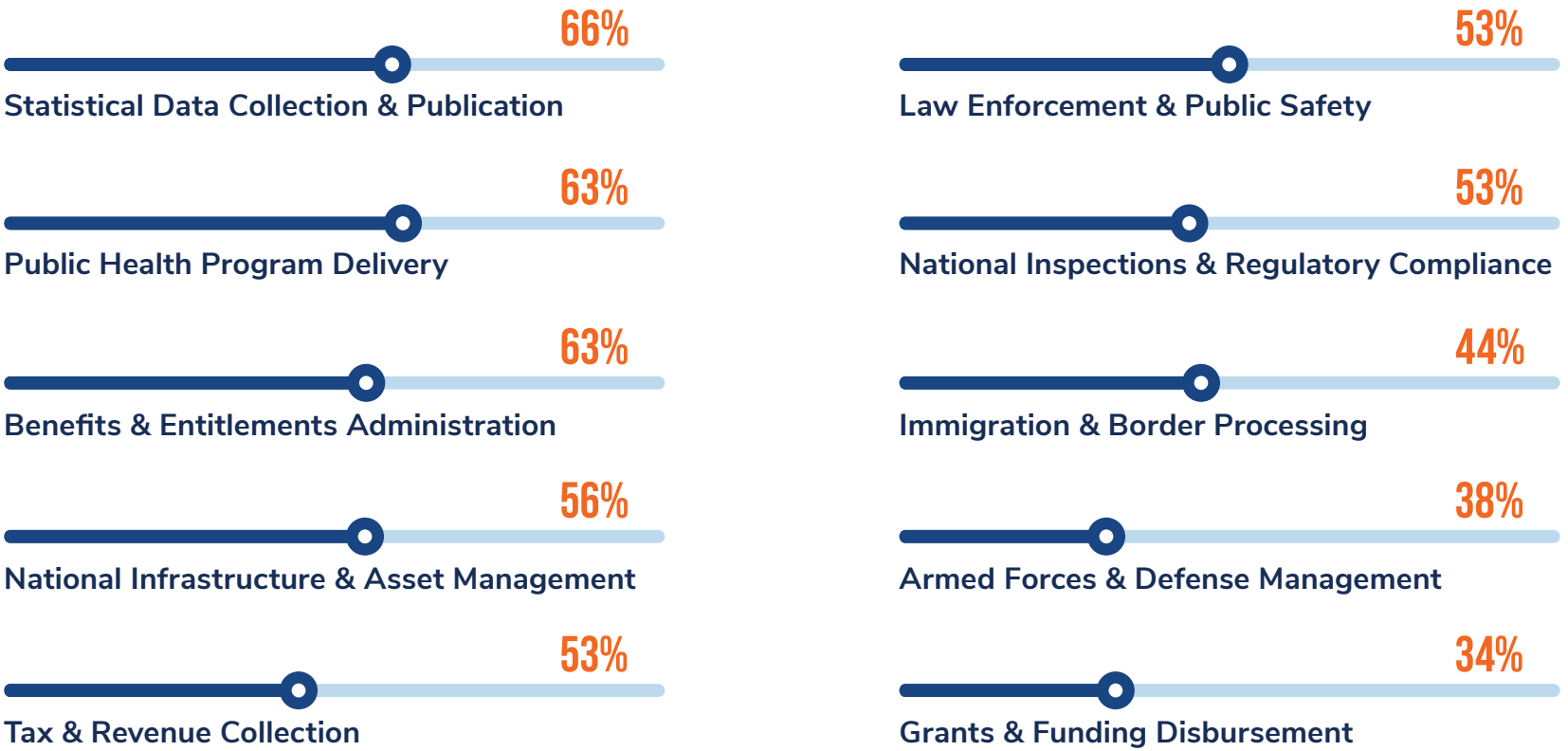
Communications Investment Determines Government Operating Capability

Viewed strategically, resilience, sovereignty, workforce transformation, hybrid architecture, and AI adoption are often planned and funded as separate modernization initiatives, each supported by its own business case and competing for budget. Yet from an operational perspective, these priorities converge on a common dependency - the communications infrastructure. This shared foundation shapes how securely, reliably, and rapidly governments can coordinate work, deliver services, manage risk, and adapt under pressure.

For national and federal government IT leaders, communications budget decisions are no longer just cost considerations. Rather than being an isolated technology layer, communications infrastructure represents a set of interconnected constraints that ultimately determine the effectiveness of every modernization effort. Choosing to maintain or expand these investments reflects a deeper understanding that reliable, secure, and scalable systems are the backbone of both service workflows and the broader digital modernization efforts that will define the future operating capability of government.



National and federal government IT decision-makers plan to invest in digital communications tools to improve workflow efficiency across the following departments over the next three years.



Communications infrastructure is now the operating layer through which government executes policy, delivers services, and coordinates response. This is just as critical in front line services as back office, such as in public safety and law enforcement, where systems built for everyday service delivery must hold firm the instant a crisis begins.

Complexity Has Become the Next Modernization Constraint

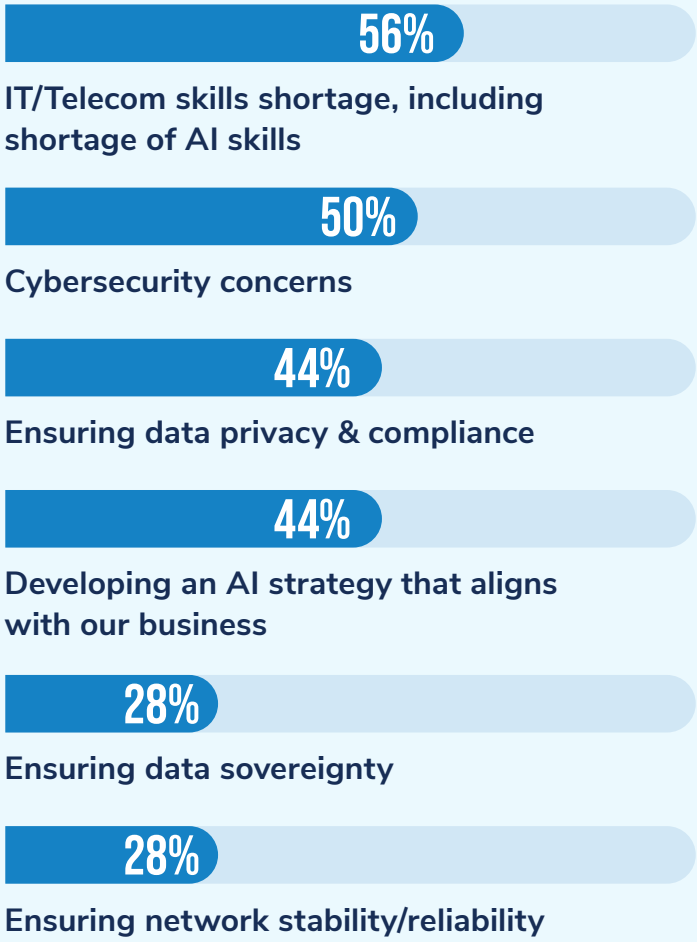
Government modernization programs have historically been defined by the challenges of funding transformation programs, selecting platforms, and deploying infrastructure. Today's infrastructure presents a different challenge, one of managing operational complexity.

While many agencies have modernized technology environments, few have modernized the operating models required to continuously govern, optimize, secure, and evolve those environments.

As a result, management constraints increasingly become the limiting factor in modernization. The challenge is maintaining operational excellence across a growing portfolio of interconnected capabilities. As a solution, managed services are evolving from a cost-management tool into a strategic operating model that provides access to specialized expertise while allowing government organizations to retain control, governance, and accountability.

The next-generation modernization challenge is not building modern communications environments. It is continuously governing them.

The range of significant challenges facing national and federal government IT decision-makers is daunting, and there are no easy fixes. A notable percentage of government IT decision-makers view the following as a significant challenge for their department over the next three years.



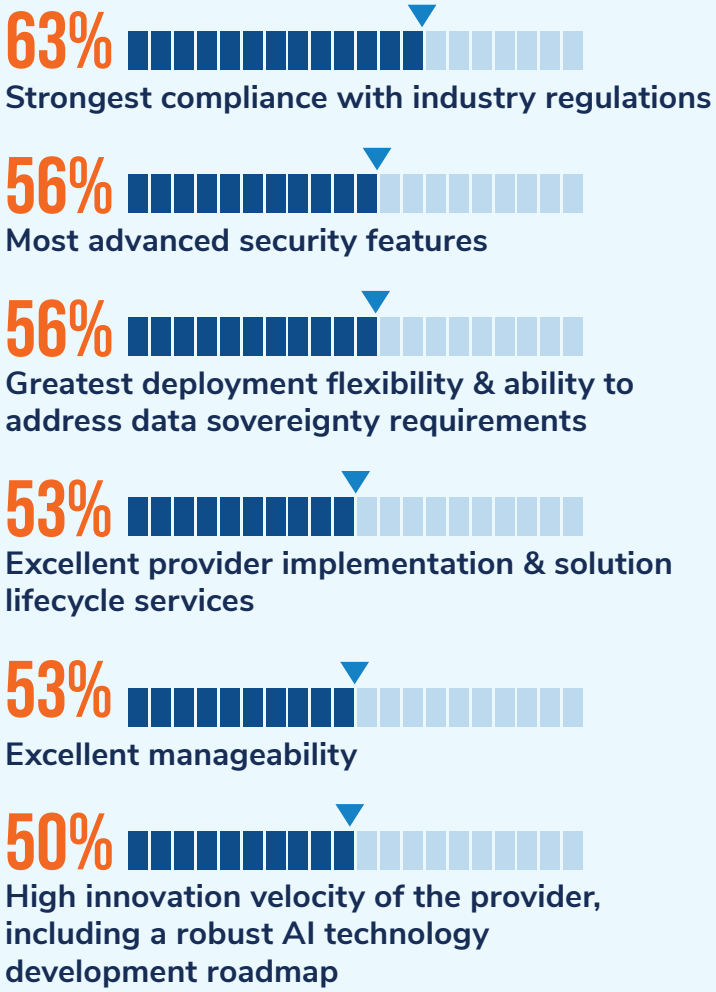
Choosing the Right Partner for Scalable, Secure Transformation

Selecting the right partner is essential for driving successful communications transformation in national and federal government organizations. With increasing pressure to modernize infrastructure, reduce complexity, and improve citizen outcomes, partner selection becomes less about technology acquisition and more about risk management.

By partnering with providers who understand the unique challenges of national and federal government organizations, IT decision-makers can deploy communication and collaboration tools that enhance staff efficiency, support evolving citizen needs, and strengthen data sovereignty and protection. Agencies are no longer purchasing individual communications products. They are selecting partners that will influence the pace, risk profile, and sustainability of modernization going forward.

Government organizations are not selecting a communications provider. They are selecting an operating partner for long-term modernization.

In practice, selecting a communications partner has become a decision about where operational risk will reside and how effectively it can be managed over time. Government IT decision-makers are now prioritizing the following from their partners:



Mitel in Practice:

Powering National and Federal Government Communication Transformation

Modernizing government requires balancing competing operational demands. Because these competing priorities represent permanent operating conditions, modernization strategies must be built around them, not despite them.

Tool sprawl forces manual coordination Disconnected voice, video, and messaging push the coordination burden onto people.	*Mitel unifies voice, video, and messaging into one platform so coordination happens by design.*
Resilience gets tested by real failure In public safety and dispatch, seconds decide outcomes.	*Mitel delivers survivable, mission-critical architecture built for real-world adversity.*
Modernization has to preserve control Hybrid estates reconcile sovereignty, continuity, and resilience with cloud innovation.	*Mitel's hybrid architecture lets government modernize at its own pace.*
Complexity outpaces internal capacity Scarce IT teams need operating models that simplify support and sustain continuity.	*Mitel simplifies operations so IT teams stay focused on public service delivery.*

Mitel helps national and federal government organizations reconcile continuity and transformation, enabling intelligent, optimized workflows that improve responsiveness and deliver consistent, citizen-centered experiences.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN

All rights reserved ©2026 Frost & Sullivan